UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE RELEASE OF HISTORICAL CELL-SITE INFORMATION.	**MEMORANDUM AND ORDER** 10-MJ-0550 (JO)

----------X

JAMES ORENSTEIN, Magistrate Judge:

The United States seeks an order pursuant to 18 U.S.C. § 2703(c)-(d) (the "Stored Communications Act" or "SCA"), directing Sprint Nextel to disclose, with respect to all calls and text messages to and from a certain mobile telephone over a period of 58 days, all "recorded information identifying the base station towers and sectors that received transmissions from" that telephone. Docket Entry ("DE") 1 at 1.[1] The government has proffered "specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation." *Id*. ¶ 2. The government also takes the position that the proffered facts establish "probable cause" sufficient to permit the issuance of a warrant for historical cell-site information pursuant to Federal Rule of Criminal Procedure 41, *id*. at 2 n.1, but it nevertheless has expressly declined to seek such relief, preferring instead to rely exclusively on the SCA. For the reasons set forth below, I deny the government's application on the ground that the Fourth Amendment requires the government to obtain a warrant, based on a showing of probable cause on oath or affirmation, in order to secure the information it seeks.

---

[1] As the caption suggests, the information at issue is commonly referred to as "historical cell-site information." Following that usage, I will use "cell-site information" or "CSI" to refer to information identifying the base station towers and sectors that receive transmissions from a mobile telephone. CSI can be either "historical" (by which I refer to information generated by communications that have already occurred at the time of the order authorizing the disclosure of such data) or "prospective" (referring to information generated by communications that have not yet occurred at the time of the order authorizing the real-time collection of such data).

I. Background

A. The Instant Application

On August 16, 2010, the government submitted an *ex parte* application for historical CSI for the period from May 1 through June 27, 2010, for a telephone issued by service provider Sprint Nextel to a subscriber named Edwin Espinosa ("Espinosa"), but actually used by the target of a continuing criminal investigation named Tyshawn Augustus ("Augustus"). Application at 1 & ¶¶ 3-4. The application relied exclusively on the SCA as authority for the requested relief, and purported to do no more than proffer "specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation." Application ¶ 2 (citing 18 U.S.C. § 2703(d)). After I expressed concern to the applicant that recent case law, as discussed below, might instead require a showing of probable cause to satisfy the Fourth Amendment, the government submitted a revised application that differed from its predecessor only by including the following disclaimer: "Although not required, the government submits that the facts set forth herein provide ... probable cause." DE 1 (revised Application) ¶ 2 n.1.[2]

The government's assertion did not alleviate my concern. Even assuming that the facts proffered in the revised Application sufficed to establish probable cause, those facts could not simply be proffered but would instead have to be established by means of an affidavit or affirmation. *See* U.S. Const. Amend. IV ("no Warrants shall issue, but upon probable cause,

[2] The original Application has not yet been filed on the docket. The government filed its revised Application on the electronic docket after I determined that I would need to reflect on the request. In doing so, it did not seek to file its revised Application under seal, and is apparently content to have its details made public, in part because, as the document reveals, Augustus is already in custody. *See id*. ¶¶ 13-14.

supported by Oath or affirmation"). I so informed the applicant and invited him to cure that defect. After consulting with his colleagues in the United States Attorney's Office, the applicant informed me that the government preferred to rely exclusively on the authority of the SCA. I therefore requested the government to submit a letter brief in support of its position that, notwithstanding recent case law, its request for relief is consistent with the Fourth Amendment. The government did so on August 19, 2010. DE 4 (the "Letter").[3]

B. The Changing Legal Landscape

I have previously granted requests similar to the one I now deny. Notwithstanding my view that the relevant statutes require an application for *prospective* CSI to establish probable cause, *see In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. And/or Cell Site Info.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) ("*CSI: Central Islip II*");[4] *but*

[3] A separate concern was that the facts proffered in the Application – as opposed to its conclusory assertions about what investigators believe – did not establish any reason to think that Augustus was using the subject telephone. The applicant told me, and has since proffered in the Letter, that a reliable confidential information had provided just such information to the New York City Police Department. *Id*. at 2 n.3. Between that assertion and those proffered in the Application, I am satisfied that probable cause exists to believe that Augustus used the subject telephone in the course of the crimes under investigation and that the historical CSI the government seeks would reveal evidence of his commission of such crimes. The only remaining impediment to granting the government the relief it seeks is therefore its unwillingness to submit the available facts in the form of an affidavit or affirmation so as to obtain a warrant pursuant to the Fourth Amendment and Federal Rule of Criminal Procedure 41 rather than pursuant to the SCA.

[4] Because many of the decisions analyzing the issues before me have long titles that resist distinctive abbreviation, in the interest of brevity I will dispense with the full captions of such cases entirely, and cite them using the following convention: "*[type of location tracking (e.g., CSI)]: [City of issuing court]*." Where necessary to distinguish cases that would have the same title using that convention, I will append to the shorthand name of the case either the year of the decision or, if necessary to distinguish cases decided in the same year, Roman numerals.

see, *e.g.*, *CSI: Brooklyn*, 632 F. Supp. 2d 202 (E.D.N.Y. 2008); *CSI: New York*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); I have previously concluded – and continue to believe – that as a statutory matter the SCA permits a court to issue the order the government now seeks without a showing of probable cause. *See CSI: Central Islip II*, 396 F. Supp. 2d at 397 n.10 (citing *CSI: Houston (2005)*, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005)); *see also United States v. Benford*, 2010 WL 12666507 (N.D. Ind. Mar. 26, 2010); *CSI: Boston*, 509 F. Supp. 2d 76 (D. Mass. 2007) (reversing 509 F. Supp. 2d 64 (D. Mass. 2007) (decision of magistrate judge)); *United States v. Suarez-Blanca*, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008); *but see CSI: Pittsburgh*, 534 F. Supp. 2d 585 (W.D. Pa. 2008), *aff'd on motion for reconsideration by district judge*, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (appeal pending); *CSI: Austin,* 2010 WL 3021950 (W.D. Tex. July 29, 2010); *CSI: Fort Wayne*, 2006 WL 1876847 (N.D. Ill. July 5, 2006).[5]

---

[5] As the foregoing citations suggest, the case law is unsettled on a variety of substantive and procedural issues relating to the use of location tracking as an investigative technique. *See generally*, *Hearing on Elec. Commc'ns Privacy Act Reform & the Revolution in Location Based Techs. & Servs. Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, S. Comm. on the Judiciary*, 111th Cong. (statement of Stephen Wm. Smith, U.S. Mag. J., at 3-7 & n.14) (June 24, 2010), *available at* http://judiciary.house.gov/hearings/pdf/Smith100624.pdf ("Smith Hearing Testimony") (summarizing inconsistent decisions and general absence of appeals); *id*. at Ex. B (summary of decisions on various issues involving CSI).

That case law remains unsettled primarily for two reasons. First, although location tracking can sometimes provide actual evidence of a crime, in many instances the government seeks such information merely because it will lead to such evidence. *See*, *e.g.*, *CSI: Washington*, 407 F. Supp. 2d 132 (D.D.C. 2005). In addition, applications and orders for CSI often remain under seal long after any legitimate need for secrecy has dissipated. *See* Smith Hearing Testimony at 9-12. As a result, investigative targets usually lack notice of or standing to appeal decisions granting access to CSI. Second, while the government unquestionably knows when its requests are denied, and just as unquestionably has standing to seek review of such denials, it has (with one exception in the Third Circuit) steadfastly chosen to avoid seeking such review.

The result, in this circuit and others, has been an unpredictable legal regime in which an individual's right to privacy waxes and wanes based on the fortuity of the location in which an

Statutory authority, of course, is not sufficient if such authority purports to allow, without a showing of probable cause, a search or seizure that must be considered unreasonable under the Fourth Amendment.[6] I have not previously balked at issuing orders to disclose historical CSI on a showing of "specific and articulable facts" pursuant to the SCA in large part because, until now, the federal appellate courts to have addressed the issue have uniformly interpreted *United States v. Knotts*, 460 U.S. 276 (1983), to hold that location tracking outside the home is analogous to physical surveillance and therefore does not require a warrant. *See United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010); *United States v. Pineda-Moreno,* 591 F.3d 1212 (9th Cir. 2010), *reh'g en banc denied*, --- F.3d ----, 2010 WL 3169573 (9th Cir. Aug. 12, 2010); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007).

That uniformity no longer exists. The United States Court of Appeals for the District of Columbia Circuit recently reversed the conviction of a defendant on the ground that evidence obtained in violation of his rights under the Fourth Amendment had improperly, and

---

investigation is based and of each district court's system for assigning miscellaneous criminal duty to its judges. It is a regime in which prosecutors, rather than seeking to establish predictable legal norms, understandably "tend to gravitate toward a judge who is known to view their requests less critically." Smith Hearing Testimony at 12.

[6] I recognize that the foregoing statement is in some sense a tautology. An unreasonable search for purposes of the Fourth Amendment is one that intrudes on an expectation of privacy that society is prepared to recognize as reasonable – and legislation is plainly a vehicle for society to grant, or deny, such recognition. Accordingly, to be more precise, the federal statutes governing electronic surveillance and privacy do not *explicitly* address the circumstances in which the government may deploy location tracking technologies. *See generally CSI: Houston (2005)*, 396 F. Supp. 2d at 761-65 (reviewing statutory scheme and analyzing government's claim that authority for warrantless collection of prospective CSI arises from the interaction of several statutory provisions enacted over a period of 26 years). Thus, whatever the best reading of the SCA, it is manifest that Congress did not purport in enacting that law to definitively accept or reject the reasonableness of any particular expectation of privacy with respect to location tracking – and that therefore the statute is not immune to Fourth Amendment scrutiny.

prejudicially, been admitted at trial. The investigating agents obtained such evidence by surreptitiously, and without a valid warrant, installing on the defendant's vehicle a global-positioning-system ("GPS") device that allowed them to track the location of that vehicle continuously for a month. *See United States v. Maynard*, --- F.3d ----, 2010 WL 3063788, at *7-*18 (D.C. Cir. Aug. 6, 2010). In reaching its decision, the court explained in detail why it was not foreclosed by the result or the reasoning in *Knotts* – to the contrary, the court explained how the *Knotts* opinion had refrained from holding that *prolonged* warrantless location tracking was consistent with the Fourth Amendment. *See id*. at *8-*9; *see also Pineda-Moreno*, 2010 WL 3169573, at *4 (Kozinski, C.J., dissenting) (similarly distinguishing *Knotts*).

The decision in *Maynard* is just one of several rulings in recent years reflecting a growing recognition, at least in some courts, that technology has progressed to the point where a person who wishes to partake in the social, cultural, and political affairs of our society has no realistic choice but to expose to others, if not to the public as a whole, a broad range of conduct and communications that would previously have been deemed unquestionably private. *See Maynard*, 2010 WL 3063788, at *13 & n.*, *15 (noting that pattern of movements over prolonged period, including to places such as church or doctor's office, reveals "intimate portrait" of subject's life and that cost and effort to deploy and continue using GPS surveillance is insignificant, and concluding that "the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave"); *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007) (holding that an individual's reasonable expectation of privacy in the content of email communications is not vitiated by an understanding that the third-party service provider will maintain independent access to them, noting that electronic communication "is as

important to Fourth Amendment principles today as protecting telephone conversations has been in the past"), *vacated en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008); *CSI: Pittsburgh*, 534 F. Supp. 2d at 610-16 (concluding that interpreting the SCA to allow disclosure of historical CSI without a showing of probable cause renders the statute constitutionally suspect); *see also Pineda-Moreno,* 2010 WL 3169573, at *7 (Kozinski, C.J., dissenting) ("There is something creepy and un-American about such clandestine and underhanded [continuous surveillance].... Some day, soon, we may wake up and find we're living in Oceania.").

As a result of such decisions, I believe that magistrate judges presented with *ex parte* requests for authority to deploy various forms of warrantless location-tracking must carefully re-examine the constitutionality of such investigative techniques, and that it is no longer enough to dismiss the need for such analysis by relying on cases such as *Knotts* or, as discussed below, *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that telephone users have no expectation of privacy in dialed telephone numbers because they voluntarily expose such information to the service provider).[7] For the reasons discussed below, I now conclude that the Fourth Amendment prohibits as an unreasonable search and seizure the order the government now seeks in the absence of a showing of "probable cause, supported by Oath or affirmation[.]" U.S. Const. Amend. IV.

---

[7] The circuit court decisions considering the application of *Knotts* to modern location-tracking technology all involved the remote surveillance of an investigative subject's location by means of a GPS tracking device surreptitiously placed on the subject's vehicle. As far as I am aware, no circuit court has yet addressed the constitutional issue in the context of any form of location tracking of a subject's mobile telephone. Such a case is currently pending in Third Circuit as a result of the government's appeal of the district court's affirmance of the magistrate judge's decision in *CSI: Pittsburgh*.

II. Discussion

A. *Maynard*: The "Intimate Picture" Rationale

The *Maynard* court, in holding that warrantless GPS tracking over the course of a month constituted a search, acknowledged that the federal appellate courts in three sister circuits had reached a contrary conclusion under the Supreme Court's decision in *Knotts*. *Id.* at *9 (citing *Marquez*, 605 F.3d 604; *Pineda-Moreno,* 591 F.3d 1212, *reh'g en banc denied* --- F.3d ----, 2010 WL 3169573; *Garcia*, 474 F.3d 994). In *Knotts*, the police had used a "beeper" (a form of transmitter) to track a vehicle's progress as it moved from one place to a destination approximately 100 miles away. *Knotts*, 460 U.S. at 277. The Supreme Court held that there had been no search because the subject, driving on public roads, "voluntarily conveyed to anyone who wanted to look" his progress and route, so he could not reasonably expect privacy in "the fact of his final destination." *Id.* at 281-82.

While the appellate courts in *Marquez*, *Pineda-Moreno*, and *Garcia* all held that *Knotts* compelled the finding that prolonged GPS surveillance was not a search, the *Maynard* court disagreed. It persuasively explained that the Court in *Knotts* "explicitly distinguished between the limited information discovered by use of [a] beeper – movements during a discrete journey – and more comprehensive or sustained monitoring of the sort at issue in [*Maynard*]." 2010 WL 3063788, at *8 (citing *Knotts*, 460 U.S. at 283-85). As the *Maynard* court demonstrated, the other cases involving GPS tracking had all rested on the mistaken understanding that *Knotts* reserved judgment only as to "whether 'wholesale' or 'mass' electronic surveillance of many individuals requires a warrant," and that, to the contrary, "the Court actually reserved the issue of *prolonged* surveillance." *Id.* (emphasis added). In particular, the *Knotts* Court rejected the

respondent's concern that its decision would necessarily lead to the possibility of "twenty-four hour surveillance of any citizen of this country ... without judicial knowledge or supervision[.]" 460 U.S. at 283 (internal quotation marks omitted). To the contrary, the Court wrote that "if such dragnet type law enforcement practices ... should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

Having established that *Knotts* did not compel it to reject the defendant's Fourth Amendment claim, the *Maynard* court proceeded to analyze whether the defendant had an expectation of privacy in the pattern of his movements over time that society recognizes as reasonable. 2010 WL 3063788, at *10 (citing *Kyllo v. United States*, 533 U.S. 27 (2001) (citing test from *Katz v. United States*, 389 U.S. 347 (1967)). The court noted that the Supreme Court's application of *Katz* precluded there being any reasonable expectation of privacy in information that was knowingly exposed to the public, but it explained that "[i]n considering whether something is 'exposed' to the public as that term was used in *Katz* we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do." *Id.* Applying that principle, the court wrote,

> [W]e hold that the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.

Id. at *12.

The court also addressed whether the defendant had constructively exposed the pattern of his movements over the month by having conducted each individual movement in public view. *Id.* at *12-*14. The court found that prolonged surveillance reveals information that differs in kind, not just in degree, from the results of any short-term surveillance. For example, while a single visit to a particular location might not reveal much, a pattern of visits would reveal if a person "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." *Id.* at *13. Indeed, the court noted that the government had made the pattern of the defendant's movements, as opposed to any one movement, central to its case, reinforcing the distinctive quality of such a collection of data. *Id.* at *13 n.*. The court found that "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain disconnected and anonymous." *Id.* at *14 (internal quotation marks omitted). Thus, the court found no constructive exposure of the pattern of movements.

Reasoning that prolonged GPS monitoring of a person's car travels reveals a picture of his life so intimate that he expects no one except perhaps his spouse to have it, the court held that the defendant's expectation of privacy in such information was reasonable. *Id.* at *14; *see also id.* at *15 (collecting, as indicative albeit non-conclusive evidence of societal understandings, statutes from eight states that impose penalties for use of electronic tracking devices and expressly exclude evidence produced by such devices unless obtained by police pursuant to warrant).

I find the opinion in *Maynard* persuasive, both with respect to its demonstration that *Knotts* is not dispositive on the issue of prolonged location tracking, and with respect to its analysis of the privacy interest at stake when the government uses technological means to accomplish the kind of prolonged, continuous, and detailed surveillance that would otherwise be impossible.[8] I therefore proceed to consider whether the *Maynard* court's reasoning applies with equal force in the circumstances of this case.

There are four primary factual differences between the real-time GPS vehicle tracking at issue in *Maynard* and the instant application for access to historical CSI records of a mobile telephone. First, in *Maynard* the government tracked the defendant's movements in real time; here, they seek information about Augustus's past movements. Second, the investigation in *Maynard* involved surveillance rather than disclosure: agents tracked their subject, albeit remotely, by means of technology in their own hands; here, by contrast, the government seeks only access to records created and maintained by a third-party service provider. Third, the GPS technology used in *Maynard* allowed for greater precision than the CSI requested here – a distinction that is heightened by the fact that the government anticipates obtaining only "single

---

[8] The government asserts that it views *Maynard* as "wrongly decided[,]" Letter at 5 n.5, but does not explain why. In lieu of argument on that point, it invites me to "*[s]ee generally United States v. Jesus-Nunez*, 2010 WL 2991229 (M.D. Pa. July 27, 2010) (denying motion to suppress GPS data)." Letter at 5 n.5. The citation to a district court decision issued in before the circuit court's ruling in *Maynard* plainly provides no basis for viewing the latter as incorrect. Moreover, the opinion in *Jesus-Nunez* proceeds from an assumption that *Maynard* conclusively demonstrates to be simply false when it begins its analysis with the observation that "Defendant candidly admits the applicability of" *Knotts*. 2010 WL 2991229, at *2. Neither the district court in *Jesus-Nunez*, nor the government here, makes any effort to explain why *Knotts* should affect the analysis of an issue it explicitly avoided discussing – namely, the Fourth Amendment implications of using technology to accomplish the *continuous* tracking of a person's movements. At any rate, the government allows that I "need not evaluate *Maynard* on its own merits ... to rule on this application." Letter at 5 n.5.

tower" CSI (as opposed to "multiple tower" CSI that permits triangulation). Fourth, the investigators in *Maynard* tracked their subject by locating his car; here, by contrast, the agents seek to learn about their subject's movements by obtaining information about the location of his mobile telephone. I address each difference in turn, as well as certain additional distinctions that the government proffers in support of its application. As explained below, I conclude – albeit with no small amount of hesitation – that none of those differences renders *Maynard* inapposite.

B. The Difference Between Historical And Prospective Location Tracking

The government first tries to distinguish *Maynard* on the ground that in the latter case, "law enforcement officers caused data to be created that would not otherwise have existed. By contrast, in this case the government seeks access to data that a third party already created, collected and maintained in the ordinary course of its business." Letter at 4; *see also id*. (noting, in the course of a separate argument, that the requested CSI "is being sought only retrospectively"). To the extent this argument focuses on the temporal difference between prospective and historical location tracking, I am unpersuaded.[9]

The fact that the government seeks information that has already been created says nothing about whether its creator has a reasonable expectation of privacy in that information. If a law enforcement agent wants to read an individual's diary, there can be no question that the government thereby "seeks access to data that [was] already created, collected and maintained[.]"

[9] To the extent the argument rests on the difference between obtaining information directly from the investigative subject via some form of surveillance and obtaining it from a third party with whom the subject has shared it, the argument rests on firmer ground. I address, and ultimately reject, that aspect of the argument in the next section of this discussion.

I nevertheless remain confident the government would agree that the diary's author enjoys a reasonable expectation of privacy in its contents.

The distinction between retrospective and prospective application may have many implications, but providing a reason to find *Maynard* inapposite is not one of them. As the government acknowledges, a critical component of the court's rationale was the fact that the warrantless surveillance at issue revealed an "intimate picture of the subject's life[.]" *Maynard*, 2010 WL 3063788, at *13 (quoted in DE 4 at 3). The picture of Tyshawn Augustus's life the government seeks to obtain is no less intimate simply because it has already been painted.

C. The Difference Between Surveillance And Disclosure

The government argues that a critical distinction between this case and *Maynard* is the fact that here it seeks nothing from Augustus, but instead seeks information that Augustus necessarily revealed to the mobile communication service provider when he used the subject telephone. As the government notes, "the entire collection of data the government seeks has already been 'actually exposed' to a third party: Sprint Nextel." DE 4 at 4 (quoting *Maynard*, 2010 WL 3063788, at *12).[10] In so arguing, the government understandably relies on two

[10] The government does not argue that Augustus has no reasonable expectation of privacy in the subject CSI because he was using a mobile telephone subscribed to by Espinosa. That fact might serve as a complete answer to any motion by Augustus to suppress the CSI. *See*, *e.g.*, *Suarez-Blanca*, 2008 WL 4200156, at *6-7 (collecting cases); *United States v. Skinner*, 2007 WL 1556596, at *17 (E.D. Tenn. May 24, 2007) (noting that use of fictitious name is analogous to abandoning property, since withholding interest from society effectively repudiates any connection in item vis-a-vis society). But I do not think it obviates the issue before me, which is whether the pending request unreasonably intrudes on any person's reasonable expectation of privacy. By way of analogy, if Augustus left incriminating physical evidence in Espinosa's residence, he would lack standing to complain about the government's warrantless seizure of that evidence – but that would not mean that the government could obtain a warrant to seize such evidence from Espinosa's home without a showing of probable cause or consent.

decisions by the Supreme Court. In *United States v. Miller*, 425 U.S. 435 (1976), the Court rejected a Fourth Amendment challenge to a subpoena for bank records on the ground that such documents were not the respondent's "'private papers'" but were instead "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Id*. at 440 (quoted in Letter at 5 (citing also *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party ... he cannot object [on the basis of the Fourth Amendment] if the third party conveys that information or records thereof to law enforcement authorities"))). Even more closely analogous, in *Smith v. Maryland*, the Court expressed doubt that any telephone user actually harbors an expectation of privacy in the numbers dialed and ruled, in any event, that such an expectation would not be reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." 442 U.S. at 743-44. As the Court reasoned, a telephone user "voluntarily convey[s] numerical information to the telephone company" and thereby "assume[s] the risk that the company [may] reveal to the police the numbers he dialed." *Id*. at 744 (quoted in Letter at 6-7).

Maynard provides no answer to such reasoning, but other equally persuasive cases do. The decision in *Warshak* explains why a person may reasonably maintain an expectation of privacy in information about herself that she knows to be held by others, and the analysis in *CSI: Houston (2005)* demonstrates why such an expectation would be particularly reasonable with respect to the location information generated by mobile telephone usage.

In *Warshak*, the government sought an order pursuant to the SCA requiring an internet service provider ("ISP") to disclose the contents of the defendant's email communications. *Warshak*, 490 F.3d at 460. The court held that the defendant had a reasonable expectation of

privacy in the content of his emails despite his understanding that the ISP maintained independent access to those messages. *Id*. at 473. In reaching that conclusion, the court laid the groundwork for its inquiry by summarizing *Katz,* in which the Supreme Court held that telephone surveillance that intercepted the content of conversations was a search and *Smith*, in which the Court held that use of a pen register installed at the telephone company's facility was not. *Warshak*, 490 F.3d at 470. It then found that the distinction between those cases revealed that "the reasonable expectation of privacy inquiry in the context of shared communications" necessarily turns on two questions. The first inquiry identifies the particular parties with whom the communications at issue were shared and those from whom disclosure was shielded; the second considers the precise nature of the information actually conveyed to the party from whom disclosure is sought. *Id*.

With respect to the first question, the court explained that sharing information with an intermediary that merely has the ability to access the information cannot erode all expectations of privacy. As the panel observed, courts have found reasonable expectations of privacy exist in the contents of phone conversations, letters, and safe deposit boxes, despite the fact that they are accessible to, respectively, telephone companies, the Postal Service, and banks. *Id*. As to the second question, the court explained:

> Like telephone conversations, simply because the phone company or the ISP *could* access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

Id. at 471 (emphasis in original). The court found that, while there may be no reasonable expectation of privacy where an ISP's contract explicitly provided that email contents would be

regularly monitored and audited, the record before it revealed that the ISP's contract provided for access only in limited circumstances. As a result, the court found a reasonable expectation of privacy did exist. *Id.* at 473-74.[11] In vacating the decision on standing grounds, the en banc court reiterated this logic, noting the variety of privacy policies in ISP contracts and concluding that "[s]ome of these ... agreements could cast doubt on the validity of § 2703(d) in a given case; others might not." *Warshak*, 532 F.3d at 527.

Even if the reasoning in *Warshak* does not suggest a reason to view with skepticism the government's argument that any reasonable expectation of privacy disappears when information is held by a third-party service provider, such an argument is particularly ill-suited to the specific context of location tracking, as the court in *CSI: Houston (2005)* ably explained in rejecting essentially the same argument.

> The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in cell site location data, analogizing such information to the telephone numbers found unprotected in *Smith v. Maryland*, 442 U.S. 735 (1979). The Sixth Circuit rejected that analogy in *United States v. Forest*, 355 F.3d 942, 951-52 (6th Cir. 2004). Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company.... [I]t is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge. Sometimes, as in *Forest*, cell site data is triggered by law

---

[11] The court noted that automated processes the ISP might use to screen for email viruses, spam, and child pornography did not waive an expectation of privacy in the contents of messages, since the processes would not disclose the contents to any person at the ISP or elsewhere. *Id*. at 474. While I do not fully embrace that aspect of the court's reasoning – it is not obvious to me that an ISP's processes for filtering spam or child pornography would not disclose the contents of the filtered messages – my reservation on that score does not undermine the overall persuasiveness of the court's more fundamental rationale that a user of communications services can have a very reasonable expectation that the service provider's necessary access to certain otherwise private information need not expose such information to the world at large. As discussed below, third-party access to information may in some circumstances make it unreasonable to expect that such information will remain private, but it will not necessarily do so in all instances.

> enforcement's dialing of the particular number. 355 F.3d at 951. For these reasons the Sixth Circuit was persuaded that *Smith* did not extend to cell site data, but rejected the defendant's constitutional claim on the narrower ground that the surveillance took place on public highways, where there is no legitimate expectation of privacy. *Id*. at 951-52 (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983)).
>
> Further support for a recognizable privacy interest in caller location information is provided by the Wireless Communication and Public Safety Act of 1999. Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)). This legislation authorized the deployment of a nation-wide 9-1-1 emergency service for wireless phone users, called "Enhanced 9-1-1." Section 5 of the bill amended the Telecommunications Act to extend privacy protection for the call location information of cell phone users:
>
> > (f) Authority to Use Wireless Location Information.–
> >
> > For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to–
> >
> > (1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title), other than in accordance with subsection (d)(4) of this section; ...
>
> 47 U.S.C. § 222(f). In other words, location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.

CSI: Houston (2005), 396 F. Supp. 2d at 756-57.

The combined effect of *Warshak* and *CSI: Houston (2005)* persuades me that the government's reliance on *Miller* and *Smith* is misplaced. Indeed, the amendment to the Telecommunications Act mentioned in *CSI: Houston (2005)* provides an additional basis for distinguishing such case law. *Miller* involved financial records that banks stored pursuant to the

Bank Secrecy Act of 1970. In holding that an expectation of privacy in such bank records was unreasonable, the Court wrote,

> The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings."

Miller, 425 U.S. at 443 (quoting 12 U.S.C. § 1829b(a)(1)). While the Bank Secrecy Act thus expressed a legislative view that people should *not* expect to maintain privacy in financial records conveyed to banks because of the burden such privacy rights would impose on other important societal interests, the amendment to the Telecommunications Act does precisely the opposite: it expresses legislative approval for the idea that a caller should expect her location information to remain private notwithstanding the unavoidable need to share it with a third-party service provider.[12]

---

[12] To be sure, the Supreme Court went on to observe in *Miller* that it "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S. at 443 (citing *United States v. White*, 401 U.S. 745, 752 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *Lopez v. United States*, 373 U.S. 427 (1963)). If that passage from *Miller* means that there can never be a reasonable expectation of privacy in any form of information that, by its nature, must be shared to some extent with a third party to make it usable, then the government's position here is correct – but it is also irreconcilably at odds with the notion that the Fourth Amendment allows our society to continually develop and refine its definition of the privacy claims it wishes to endorse. If an explicit declaration by the national legislature that disclosing one's location information to a service provider should not be deemed to serve as consent for further dissemination of such information, it is difficult to see how our society can effectively implement a consensus to recognize as legitimate an expectation of privacy in any form of information that must be shared among private parties to be usable.

Thus, not only is it questionable to assume, as a general matter, that a person can never have a reasonable expectation of privacy in information that, by its nature, must be shared with a third-party service provider; it is particularly difficult to make that assumption with respect to mobile telephone location information. I therefore conclude that the distinction between surveillance and disclosure does not foreclose applying *Maynard* here.

D. The Difference Between CSI and GPS

The government further seeks to distinguish *Maynard* on the ground that the latter case "involved the most precise of all location information: GPS data[,]" which it contrasts with the "much less precise" CSI requested here. Letter at 4. That argument is the most intuitively appealing one at the government's disposal: to the extent the court's concern in *Maynard* was the detailed nature of the "intimate picture" of a person's life painted by GPS tracking, it would appear obvious at first blush that a less precise form of location tracking might be less troubling. The government ably highlights the intuitive appeal of that argument by going on to observe that "cell-site information is especially imprecise in an area as densely inhabited as New York City, where many buildings – and the numerous residences and businesses within those buildings – are likely to be served by a single base station tower and mobile switching center." *Id*.

The intuitive appeal of that argument, is, however, no more than that. It does not withstand careful scrutiny in the light of relevant facts about the respective precision of various forms of location tracking technology – facts that the government largely ignores.[13]

[13] I note that the SCA makes no attempt to distinguish among various forms of location tracking in granting access to such information (retrospectively) on a showing of less than probable cause – indeed, it does not even purport to differentiate records of a mobile telephone user's location from any other kind of "record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)[.]" 18 U.S.C. § 2703(c)(1). Thus,

The unstated premise of the government's argument is that location tracking by means of CSI is less of an intrusion into one's privacy because GPS tracking – and GPS tracking alone – reveals a person's *precise* location. But that is simply not true. Even if GPS technology could reveal the particular building a person had entered – and as far as I am aware, it is not so precise – in an urban setting it would not reveal which office or apartment within that building that was the subject's destination. In short, GPS tracking by itself does not necessarily reveal a subject's "[r]epeated visits to church, a gym, a bar, or a bookie[.]" *Maynard*, 2010 WL 3063788, at *13. Rather, it reveals no more than the subject's repeated visits to the vicinities of such locations – but with sufficient precision to allow investigators to piece together an intimate picture of the subject's life.

To some extent, the preceding discussion of the limits of GPS tracking is speculative. What is not speculative is that the kind of GPS tracking at issue in *Maynard* was *necessarily* imprecise, and quite possibly much less precise than the tracking at issue here. When agents used GPS to track the defendant in *Maynard*, they could learn no more than the location of his

---

any argument predicated on the relative precision of a given tracking method does nothing to validate the constitutionality of the SCA's standard of "specific and articulable facts" in the context of location tracking. Similarly, the government seeks to "clarify" its application by reporting that "Sprint Nextel, like all other [mobile communications service] providers to [its] knowledge, retains information regarding only [a] single antenna tower" for each requested communication. Letter at 2 n.1. The import of that clarification is that although the terms of the government's application would permit it to obtain, without a showing of probable cause, CSI data from multiple towers – and would therefore allow the government to triangulate the subject's location with greater precision than is possible with information from only one tower – I should rest assured that the information it will actually receive will raise less of a privacy concern. If the constitutionality of the government's application rests on that clarification – that is, if *Maynard* can be distinguished only because single-tower CSI is somewhat less precise than multiple-tower CSI – then all future applications for CSI must necessarily get bogged down in an inquiry into the precise record-keeping practices currently followed by the relevant service provider.

car. If the defendant drove to an associate's home, and parked two blocks away, the tracking information would reveal only his parking spot, not his actual destination. In contrast, when Augustus used his mobile telephone, he broadcast a signal to a cell tower no more than a few hundred feet away from his actual location – not the tower nearest to the car he may have left blocks away.[14] Nevertheless, the *Maynard* court concluded that a sufficiently large amount of information about the location of a person's car could paint an intimate picture of the person driving it – and, presumably sometimes parking it some distance from his actual destination. There is simply no reason to think that a similarly large cache of CSI data about the location of a telephone that remains on its user's person will be any less useful in painting such an intimate picture.

The government glosses over that reality in arguing that the CSI it requests "does not include any information at all about where the user was during the vast majority of the day when he was not using the Subject Telephone." Letter at 5. In so arguing, the government blithely ignores that the GPS tracking of the *Maynard* defendant's car likewise did not reveal "any information at all about where [he] was during the vast majority of the day when he was not" driving.[15]

---

[14] As of February 2008, CSI from multiple towers could reveal the location of a cell phone to within approximately 50 feet, and information from a single tower to within a few hundred feet. *CSI: Pittsburgh*, 534 F. Supp. 2d at 602.

[15] Moreover, while the latter statement is unquestionably true about the defendant in *Maynard*, the former is just as plainly false about the application here. The government's application, by its explicit terms, seeks information about Augustus's location not only at the times he affirmatively chose to use his phone to make a call, but also when he passively received calls and – even more inconsistent with the government's argument – at times when that phone received text messages without any voluntary action by Augustus at all. Further, the *Maynard* defendant could only be tracked in his travels from one location to another to the extent he undertook those travels in a

At an even more basic level, the government's argument about the relative imprecision of CSI tracking ignores how much more precise such tracking has become in recent years. When the Supreme Court in *Knotts* took care to leave open the possibility that continuous location tracking over a lengthy period could constitute an unreasonable search, 460 U.S. at 283-84, it was contemplating the use of a "beeper" that used essentially the same mechanism as today's CSI tracking – and possibly with far less precision. *See Pineda-Moreno*, 2010 WL 3169573, at *4 (Kozinski, C.J., dissenting) ("The [CSI and GPS] electronic tracking devices used by the police in this case have little in common with the primitive devices in *Knotts*."); *see also CSI: Houston (2005)*, 396 F. Supp. 2d at 754 (explaining, in part on the basis of material published by the United States Department of Justice, how "beepers on vehicles are now monitored via radio signals using the very same cell phone towers used to transmit cell site data" and noting that as a result of "this convergence in technology, the distinction between cell site data and information gathered by a tracking device has practically vanished").[16]

Finally, in seeking to distinguish *Maynard* on the ground that CSI tracking is not very precise, the government proves too much. The only reason the government wants access to the

---

particular car. In contrast, the CSI the government seeks here would reveal the subject's location regardless of his mode of travel. It would therefore be capable of revealing a broader range of the subject's destinations than could the GPS vehicle tracking at issue in *Maynard*.

[16] Even if the government's argument about the relative precision of CSI and GPS tracking were more persuasive, it would do no more than carry today's argument, and postpone for a brief time the decision that would have to be made when cell towers become even more ubiquitous than they are now and the software providing location information based on CSI permits even greater tracking precision. *See CSI: Houston (2005)*, 396 F. Supp. 2d at 755 & n.11 (explaining how the "inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year"). Such an argument assures virtually instant obsolescence to a decision here in the government's favor.

CSI at issue here is that it believes such data will provide meaningful information about Augustus's past movements, even if only by means of his proximity to a specific cell tower at a given time. *See* DE 1 ¶ 3 (asserting that "the information likely to be obtained is relevant to an ongoing criminal investigation" and "will ... corroborat[e] other information concerning the location of Augustus"); *cf. Maynard*, 2010 WL 3063788, at *13 n.* (noting that government made pattern of movements, as opposed to any one movement, central to its case).

The government cannot have it both ways. If proof of Augustus's mere proximity to a specific cell tower at a specific time does *not* convey meaningful information about his precise location, then the government's certification for purposes of obtaining such information pursuant to the SCA should be rejected as false. But if that certification is true, as I am confident it is,[17] the government cannot be heard to disavow the logical import of that certification simply to avoid scrutiny under the Fourth Amendment.[18]

---

[17] To be clear, I do not mean to suggest that I entertain the slightest doubt about the sincerity of the government's certification. I have the highest confidence in the integrity of both the individual prosecutor who submitted the instant application and the United States Attorney's Office he serves. In noting the tension between the government's certification of relevance and its argument based on the limits of CSI technology, I intend only to illustrate what I perceive to be a logical fallacy of the latter.

[18] Indeed, the tension between the government's certification of relevance for purposes of the SCA and its argument about the limits of CSI technology undermines not only the government's argument about the technological difference between various kinds of tracking, but also its argument that historical tracking data should deserve less protection under the Fourth Amendment than prospective tracking. The government may have a legitimate use for prospective CSI even if such data conveys *no* useful information about a subject's precise location: a person's proximity to a given cell site, as such, may ease the task of commencing or continuing physical surveillance, or it may assist in the hunt for a fugitive. But historical CSI can serve no such function of which I am aware – with the exception of using it to disprove an alibi (an application not at issue here), information that a person was previously in proximity to a cell site is useful only to the extent it conveys information about the subject's actual location.

E. The Difference Between Vehicle Tracking And Telephone Tracking

One more potential basis for distinguishing *Maynard* from this case is that people may have a lesser expectation of privacy with respect to the location of their mobile telephones than with respect to their cars. In that vein, the government argues that "[t]he user of the Subject Telephone knows or should know that every time he places or receives a call Sprint Nextel is advised of the cell tower being used, because the user knows that Sprint Nextel may later charge him for its services based in part on his location." Letter at 4-5.

The government provides no factual basis for that assertion, and it strikes me as being not only unsupported but, in recent years, unsupportable. In years gone by, when a brick-sized "mobile" telephone could not fit in the average pocket or purse, the monthly bill for cellular service typically included charges based to some extent on the location of the user's telephone during each call made or received. In recent years, however, I am under the impression that most mobile telephone subscribers pay a flat fee (on a one-time or monthly basis) for a specific number of minutes of call time (or a specific number of text messages), regardless of location. *See CSI: Pittsburgh*, 534 F. Supp. 2d at 590 n.20 (noting that "the advent of truly national networks and comprehensive cell phone 'plans'" has made location "increasingly irrelevant to service fees"). If that is correct, then there would be no reason – at least none based on expectations about billing – for a mobile telephone user to think the service provider would maintain records of the locations of her calls.

I need not inquire further into that factual matter because I do not assume that persons who use mobile telephones are unaware of the fact that by doing so they expose themselves to location tracking. Indeed, with the growing availability and popularity of commercial

applications that allow a mobile telephone user to affirmatively broadcast her location, I assume that most people are – or will soon be – aware of that fact. But that assumption does not preclude reliance on the conclusion in *Maynard* that people in this country have a reasonable expectation of privacy in their movements over extended periods of time. To the contrary, I believe that a growing awareness of the *possibility* of location tracking of mobile telephones has also produced a growing expectation that such tracking can and should be controlled.

It is increasingly common for mobile telephone subscribers to make affirmative use of location tracking by subscribing to premium telephone services or independent location-based applications. The providers of both routinely address – and try to alleviate – their customers' concerns about the unintended dissemination of information about their location. For example, Verizon Wireless assures its subscribers that it "understands that advances in wireless technology, especially the growing availability of location-based services, bring new concerns about how customer information is used and shared." It provides its customers with "clear notice regarding how these types of services work and require that they make the choice about whether specific location-tracking features available on their phones are turned on when using their wireless phones." The company goes on to assert that its customers "are given the opportunity to choose where and when to turn specific location-based services on and off." Verizon | About Verizon – Privacy Policy, http://www22.verizon.com/about/privacy/policy/#wireless (last visited Aug. 27, 2010); *see also* AT&T Privacy Policy, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Aug. 27, 2010) (noting that cell-site information is used "to provide your wireless service" while location information for other services "will be used ... only with prior notice and your consent").

Similarly, a popular mobile telephone application called "foursquare" permits users to share their location to facilitate connections with friends by "checking in" at a given location, such as a bar or restaurant, and seeing other users of the same service who are currently or were previously "checked in" to that location. The company takes pains to acknowledge that "an important concern for most anyone using location-based services is privacy" and strives to make its subscribers "comfortable with how [location-tracking] information is shared via foursquare." To that end it boasts of creating "a range of robust privacy controls [that] give users control over the amount of information they share about their location." Those controls ostensibly empower a user to have her "entire check-in history ... removed from [the company's] database." Foursquare, http://foursquare.com/privacy/ (last visited Aug. 27, 2010); *see also* Google Latitude, http://www.google.com/mobile/latitude/ (last visited Aug. 27, 2010) (providing application that permits mobile telephone users to share their location with friends and advertising ability to "share, set, hide your location, or sign out of Google Latitude" and to "[c]ontrol who sees your location, and at what level of detail"); *but see* Google Mobile Privacy Policy http://www.google.com/mobile/privacy.html (last visited Aug. 27, 2010) ("If you use location-enabled products and services, such as Google Maps for mobile, you may be sending us location information. This information may reveal your actual location, such as GPS data, or it may not .... Certain of our products and services allow you to opt-out of certain information gathering and sharing or to opt-out of certain products, services, or features.").[19]

[19] To be sure, conveying the message that a customer has control over certain forms of commercially available location-tracking does not necessarily suggest that she can control access to all location information. But by focusing consumer awareness on privacy concerns about location-tracking and simultaneously seeking to reassure people about that concern, the companies providing such services appear to be fostering an actual – and to my mind reasonable

Mobile telephones equipped with tracking capabilities such as GPS – the vast majority, as a result of federal law[20] – often also include features that lead the user to believe that such tracking has been disabled. Commercial location-tracking services tout their subscribers' ability to limit, or even delete, the dissemination of such information. Simply put, there is no reason to think that the advance of technology brings with it an expectation that privacy is lost; rather, I assume that it serves only to increase awareness of the importance of privacy and to whet the appetite for ways to manage it.[21]

– expectation that such information will remain private to the extent a subscriber chooses to make it so. At a minimum, it would be unreasonable to conclude, as the government contends, that mobile telephone subscribers should be aware that they cannot exercise control over access to location-tracking information generated by their mobile telephone usage. *Cf.* Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace 1, 3 (Oct. 2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf (reporting results of national survey from 2003 and 2005 showing that 59% of respondents believed fact company possessed privacy policy meant user data were not shared when in fact policies merely tell users *whether or how* such data is shared and that 85% rejected common online advertising business model when explained in simple terms).

[20] The Federal Communications Commission's Enhanced 911 Emergency Call Systems rules require a cellular service provider to equip mobile telephones with the ability to identify their locations to some degree of precision. Specifically, such telephones must be able to provide information about their location to within "50 meters for 67 percent of calls [and] 150 meters for 95 percent of calls." 47 C.F.R. § 20.18(h)(1)(ii).

[21] Two articles published in the brief period that the instant application has been pending illustrate that growing awareness and concern. The release of a new location-tracking application on the popular Facebook service led immediately to widespread interest in controlling it. *See* Farhad Manjoo, *Facebook Knows Where You Are*, Slate (Aug. 19, 2010, 4:23 PM), http://www.slate.com/id/2264492 (last visited Aug. 27, 2010). And the abstruse issue of location-tracking jurisprudence has become sufficiently important to the public at large to have been the subject of an article in a popular weekly news magazine. *See* Adam Cohen, *The Government's New Right to Track Your Every Move With GPS*, Time, Aug. 25, 2010, *available at* http://www.time.com/time/nation/article/0,8599,2013150,00.html.

F. The Government's Other Arguments

I believe that the foregoing discussion addresses as best I can (without unduly delaying the government's investigation) the strongest arguments in support of the proposition that *Maynard* does not invalidate the SCA's procedure for obtaining historical CSI on a showing of less than probable cause. In the interest of completeness, I turn to two additional arguments the government raises in its Letter.

First, the government notes that "the *Maynard* law enforcement officers covertly placed equipment upon the defendant's property in order to obtain location information. Here, the location information originated from equipment – a cell phone – that a person knowingly and voluntarily used and which equipment transmitted data as part of its normal operation." Letter at 4. The observation, while unquestionably correct, is meaningless. It is equally correct to observe that a mobile telephone user knowingly and voluntarily speaks into her device, which then broadcasts the contents of her communications as part of its normal operations. That fact plainly does not shield the contents of the broadcast communications from the protection of the Fourth Amendment's warrant requirement.

Second, the government contends that "in *Maynard* the GPS device provided data to the government 24 hours a day, allowing law enforcement officers to track the defendant in real time. Here, cell-site data exists only for the moments in time during which the phone was engaged in a call or text message transmission[.]" *Id*. This last argument is not only as meritless as its predecessor as a matter of logic, it does not even have the virtue of being factually correct. While it may be true that the GPS device in *Maynard* provided continuous data about the location of the subject's *car*, it only provided information sufficient to "track the *defendant*"

himself "for the moments in time during which" he was "engaged in" driving that car. As a practical matter, then, there is no reason to suspect that the tracking at issue in *Maynard* was in any meaningful sense more continuous than would be produced by the CSI the government seeks here. Indeed, as explained in the preceding section, tracking a vehicle may provide *less* continuous information about a subject's location than tracking his mobile telephone.

Moreover, even if the government's factual assertion were supportable, the difference between continuous location tracking and the tracking of a person's location at particular points in time is ultimately unpersuasive as a basis on which to distinguish *Maynard*. The *Maynard* court's concern with sustained GPS tracking over the course of a month was not its formally continuous nature, but rather the fact that it results in a vast collection of specific data points that, viewed together, convey the "intimate picture" of the subject's life. It is the ability to amass a collection of such points, and not the ability to trace the route from each one to the next, that carries with it the ability to resolve those points into a comprehensible picture. Thus, the fact that the government now seeks only certain data points, by itself, does not serve to distinguish the investigative technique at issue here from the one considered in *Maynard* in any meaningful way.

III. Conclusion

I recognize that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario, Cal. v. Quon*, --- U.S. ----, 130 S. Ct. 2619, 2629 (2010) (citing *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. at 353). It likewise risks error in being too reticent on that score. In particular, by waiting too long to weigh in on the constitutionality of warrantless access to newly created kinds of information, the judiciary risks

the error of transforming from mere assertion to self-fulfilling prophecy the government's contention that people categorically lack any reasonable expectation of privacy in such information.

As the Supreme Court acknowledged in *Quon* when it alluded to the progression from *Olmstead* to *Katz*, the Fourth Amendment's concept of an "unreasonable" intrusion into one's personal affairs, by its very nature, is not stuck in the amber of the year 1791. That concept must instead evolve along with the myriad ways in which humans contrive to interact with one another. As the threads that connect us are increasingly entrusted into the hands of strangers who promise to make those connections broader, more intimate, more efficient, and more productive, a jurisprudence that mechanically relies on that fact to disclaim the need for meaningful oversight of the government's investigative techniques unwisely abandons the critical and continuing task of identifying the expectations of privacy our society is prepared to recognize as reasonable.

The Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society. Because I conclude, for the reasons set forth above, that granting the government's request for warrantless access to almost two months' worth of historical cell-site location records would help to create just such a dilemma, I deny its application.

SO ORDERED.

Dated: Brooklyn, New York
August 27, 2010

/s/ James Orenstein
JAMES ORENSTEIN
U.S. Magistrate Judge